PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-337844
(43)Date of publication of application : 06.12.1994

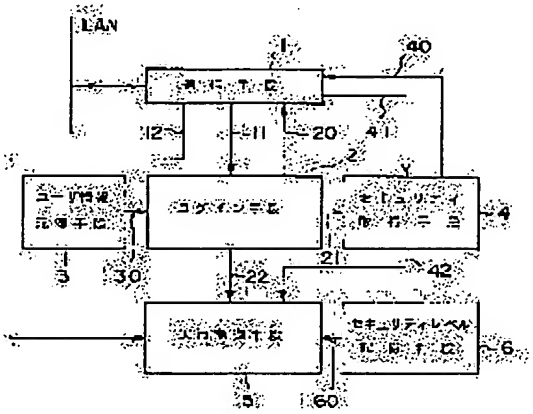
(51)Int.Cl. G06F 15/00
G06F 13/00

(21)Application number : 05-148311
(22)Date of filing : 28.05.1993

(71)Applicant : NEC CORP
(72)Inventor : OGAWA NAOTAKA

(54) LOG-IN SYSTEM

(57)Abstract:
PURPOSE: To obtain appropriate security protection corresponding to a channel by acquiring the security level of the channel from a log-in request source to a log-in destination, and deciding the propriety of the execution of a command.
CONSTITUTION: The security acquirement means 4 of the log-in destination transmits a signal inquiring the security level of the channel through a communication means 1, and transmits it to the log-in request source through a midway gateway (relay place). The respective gateways answer the security level of the channel to the next gateway to the log-in destination. The security acquirement means 4 of the log-in destination transmits the lowest level among the transmitted security levels to an execution control means 5 as the security level of the channel. The execution control means 5 compares the security level requested for the execution of the command with the security level of the channel, which is transmitted from the security acquirement means 4, and the execution of the command is permitted or the execution of the command is inhibited.



LEGAL STATUS

[Date of request for examination]	28.05.1993
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	2105027
[Date of registration]	06.11.1996
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	21.03.2002

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平６－３３７８４４

(43)公開日　平成６年（１９９４）１２月６日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
G06F 15/00	330	D 7459-5L		
13/00	351	Z 7368-5B		

審査請求　有　請求項の数２　ＦＤ　（全５頁）

(21)出願番号　特願平５－１４８３１１

(22)出願日　平成５年（１９９３）５月２８日

(71)出願人　０００００４２３７
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　小川　直孝
東京都港区芝五丁目７番１号　日本電気株式会社内

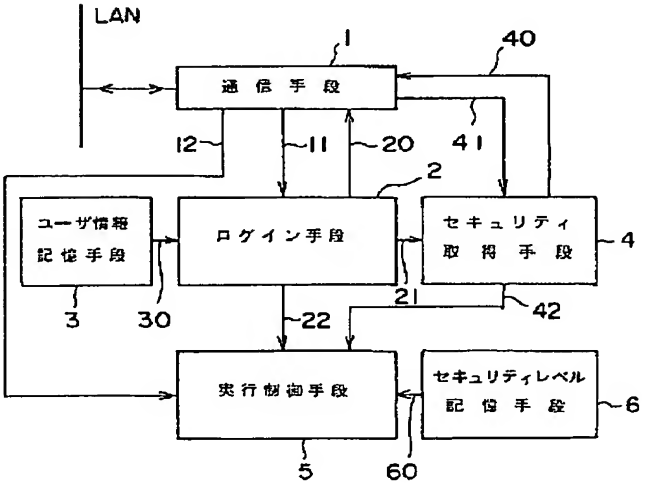
(74)代理人　弁理士　髙橋　友二

(54)【発明の名称】ログイン方式

(57)【要約】

【目的】　コンピュータシステムにおいてログインの際に使用する通信路に応じたセキュリティ保護を実行する。

【構成】　ログインを許可するログイン要求元に対してログイン先から通信路のセキュリティレベルを問い合わす問い合わせ信号を出し、この問い合わせ信号に対し通信路上の各中継所では自中継所からログイン要求元へ向けての次中継所までの通信路のセキュリティレベルを回答し、この回答が順次中継されてログイン先に送られ、ログイン先では回答されたセキュリティレベルのうちの最低のセキュリティレベルをログイン通信路のセキュリティレベルとし、コマンドの実行に要求されるセキュリティレベルと比較してコマンド実行の可否を判定した。



1

【特許請求の範囲】

【請求項１】　ログイン要求元（すなわち、ログインユーザ）から通信路を経由してログイン先（すなわち、ログイン対象のコンピュータ）にログインするログイン方式において、

上記ログイン先に設けられ、上記ログイン要求元に付与されたログイン名とそのパスワードおよび上記ログイン名に対応するセキュリティレベルを記憶するユーザ情報記憶手段、

上記ログイン先に設けられ、上記ログイン要求元から送られてきたログイン要求に付属するログイン名とそのパスワードとを上記ユーザ情報記憶手段に照合してログインの許可を判定し、ログインを許可すると判定したときはログインを許可する信号を出力するログイン手段、

このログイン手段の出力するログインを許可する信号に応じて、通信路セキュリティレベルを問い合わす問い合わせ信号を当該ログイン要求元に当て出力するよう上記ログイン先に設けられるセキュリティ取得手段、

このセキュリティ取得手段からの上記問い合わせ信号と上記ログイン手段からのログインを許可する信号とを当該ログイン要求元宛送信する通信手段、

この通信手段から送信された上記問い合わせ信号に対する回答から上記セキュリティ取得手段において上記通信路のセキュリティレベルを決定する通信路セキュリティレベル決定手段、

上記ログイン先に設けられ、コマンドの実行のために要求されるセキュリティレベルを記憶するセキュリティレベル記憶手段、

上記ログイン要求元から上記通信手段を介して入力されるコマンドに対応するセキュリティレベルを上記セキュリティレベル記憶手段から読み出し、この読み出したセキュリティレベルと上記通信路セキュリティレベル決定手段で決定された上記通信路のセキュリティレベルおよび上記ログイン名に対応して上記ユーザ情報記憶手段から読み出されたセキュリティレベルとを対照して当該コマンド実行の可否を決定する実行制御手段、

を備えたことを特徴とするログイン方式。

【請求項２】　請求項１の通信路セキュリティレベル決定手段は、

前記通信手段から前記ログイン要求信号の通進路を逆方向に通信路セキュリティレベル問い合わせ信号を前記ログイン要求元宛に送出する手段、

上記通信路上の各中継所で上記問い合わせ信号を順次中継する手段、

上記通信路上の各中継所で自局中継所から上記ログイン要求元へ向かう次中継所までの通信路のセキュリティレベルを上記通信手段宛に回答する手段、

上記通信路上の各中継所で上記通信手段宛に回答された上記通信路のセキュリティレベルを上記通信手段まで中継する手段、

2

上記通信手段が当該通信手段から当該通信手段に最も近い中継所までの通信路のセキュリティレベルと、上記各中継所で中継されて入力される各通信路のセキュリティレベルとを前記セキュリティ取得手段に転送し、上記セキュリティ取得手段がその転送されたセキュリティレベルの内の最も低い値を通信路セキュリティレベルとして前記実行制御手段へ出力する手段、

を備えたことを特徴とするログイン方式。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、コンピュータシステムのログイン（ｌｏｇ　ｉｎ）方式に関し、特にログインが通信路を介して行われる場合のセキュリティ（ｓｅｃｕｒｉｔｙ）保護に関するものである。

【０００２】

【従来の技術】ログインの対象となるコンピュータシステムでは、ログイン要求元（ログインユーザ）の種類に応じて実行可能なコマンドの種類を制限し、無資格者に対して秘匿すべき情報がその無資格者に流出したり、無資格者によって情報が破壊されたりするのを防止している。このため、ログイン要求元にはログイン名を付与し、当該ログイン要求元であることを証明するためのパスワードの入力を要求している。また、上記ログイン名に応じて実行可能なコマンドのレベルはログインの対象となるコンピュータシステム側で記憶し、ログイン要求元から入力されるコマンドをこの記憶に照らして当該コマンドの実行を許可するか否かを決定している。

【０００３】ログインは一般には通信路を介して実行されるが、通信路ではデータが盗聴される危険性があり、この危険性は通信路の種類によって異なる。従って、同一のログイン要求元であっても、それがどの通信路を経由してログインするかによって実行を許可するコマンドのレベルを変更しなければならない。従来はログイン要求元のセキューリティレベルとその要求元が通常使用する通信路のセキューリティレベルとを併せて考慮したセキューリティレベルに対応するログイン名を要求元に付与しておき、このログイン名に応じて実行を許可するコマンドのレベルを決定していた。

【０００４】

【発明が解決しようとする課題】以上のような従来のログイン方式では、同一のログイン要求元が、異なる通信路を使用してログインする場合には、通信路ごとに異なるログイン名を付与しておかねばならず、運用に混乱をきたすという問題があり、また、予め考えられていなかった通信路を使用してログインする事態が発生したとき、その通信路のセキューリティレベルは不明であり、予め定められているログイン名の内のどれかを使用してログインしたのでは適切なセキューリティ保護が得られないという問題がある。

【０００５】本発明は従来の方式における上述の問題点

3

を解決するためになされたもので、どのようなログイン要求元がどのような通信路を経由してログインした場合にも適切なセキュリティ保護を与えることのできるログイン方式を提供することを目的としている。

【０００６】

【課題を解決するための手段】本発明ではログインを認められているユーザ（ログイン要求元という）のログイン名とパスワードとそのユーザが実行することが可能なコマンドを示すセキュリティレベルを、ログインの対象となるコンピュータシステム（ログイン先という）のユーザ情報記憶手段に記憶しておき、ログイン要求元が通信路を経由しログイン名とパスワードを示してログインを要求してきたとき、ユーザ情報記憶手段の記憶と照合してログインを許可すべきか否かを判定し、ログインを許可するときは、ログイン要求元からログイン先に到る通信経路のセキュリティを取得し、実行を要求されたコマンドについて、ログイン要求元のセキュリティレベルと通信経路のセキュリティレベルとが当該コマンドに対し要求されるセキュリティレベルを満足している場合そのコマンドの実行を許すこととした。

【０００７】通信路セキュリティの問い合わせはログイン先から発せられ、ログインに使用する通信路を経由して途中のゲートウェイを介しログイン要求元に達し、各ゲートウェイは次ゲートウェイに到る（ログイン要求元に最も近いゲートウェイはログイン要求元に到る）通信路のセキュリティレベルを報告し、この報告はログインに使用する通信路によりログイン先に送られる。

【０００８】

【実施例】図１は、本発明の一実施例を示すブロック図であって、１はＬＡＮ（ｌｏｃａｌ　ａｒｅａ　ｎｅｔｗｏｒｋ）に接続された通信手段、２はログイン要求元に対しログインを許可するか否かを判定するログイン手段、３はログイン名、パスワード、セキュリティレベルが登録されているユーザ情報記憶手段、４は通信路のセキュリティを取得するためのセキュリティ取得手段、５はログイン要求元から要求されるコマンドの実行を制御する実行制御手段、６は実行制御手段５が参照するコマンドの実行に必要なセキュリティレベルを記憶するセキュリティレベル記憶手段である。

【０００９】また、１１はログイン要求元から送られてくるログイン名とパスワードの流れを示し、１２はログイン要求元から送られてくるコマンド実行要求の流れを示し、３０はログイン手段２が読み出して参照するログイン名、パスワード、セキュリティレベルの流れを示し、２０，２１はログインを許可する信号の流れを示し、２２はログイン要求元のセキュリティレベルの流れを示す。４０は通信路のセキュリティレベルを問い合わせる信号の流れ、４１はその問い合わせに対する返信の流れ、４２は通信路セキュリティレベルを示す信号の流れ、６０はセキュリティレベル記憶手段６から読み出されるセクリティレベルを示す信号の流れをそれぞれ表している。

4

【００１０】図２はログイン先（ログイン対象）、ログイン要求元（ログインユーザ）、通信路の関係を示すブロック図で、７はログイン先、８，９はそれぞれゲートウェイ（中継所）、１０はログイン要求元である。ログイン先７はＬＡＮ１に接続され、ログイン要求元１０はＬＡＮ２に接続され、ＬＡＮ１とＬＡＮ２はＷＡＮ（ｗｉｄｅ　ａｒｅａ　ｎｅｔｗｏｒｋ）に含まれ、ＷＡＮの内部でＬＡＮ１とＬＡＮ２とは、例えばゲートウェイ８，９による中継で接続される。

【００１１】次に動作について説明する。ログイン要求元１０からログイン先７に対しログイン要求を行うときは要求信号、ログイン名、パスワードが、図２に示す通信路を経てログイン先７の通信手段１を介して符号１１で示す流れにより、ログイン手段２に送られる。ログイン手段２では送られてきたログイン名とパスワードとがユーザ情報記憶手段３に登録されているか否かを調べ、登録されている場合はログインを許可し、ログイン許可を示す信号を符号２０，２１で示す流れにより通信手段１とセキュリティ取得手段４に送る。また、送られてきたログイン名に対応するセキュリティレベルをユーザ情報記憶手段３から取得して符号２２で示す流れにより実行制御手段５に送る。

【００１２】ログイン手段２から送られてくるログイン許可の信号に応じてセキュリティ取得手段４は通信路のセキュリティレベルを問い合わせる信号を符号４０で示す流れにより通信手段１に送る。通信手段１は符号２０で示す流れにより送られたログインを許可する信号と符号４０で示す流れによる通信路セキュリティレベル問い合わせ信号（以下総称して問い合わせ信号という）とをログイン要求信号の送られてきた通信路を逆順にログイン要求元１０宛に送る。この問い合わせ信号は最初にゲートウェイ８で受けられ、ゲートウェイ８はこれをゲートウェイ９に中継するとともにゲートウェイ８と９との間の通信路のセキュリティレベルをログイン先７宛に回答する。ゲートウェイ８から問い合わせ信号を中継されたゲートウェイ９は、これをログイン要求元１０へ中継するとともにゲートウェイ９からログイン要求元１０までの通信路のセキュリティレベルをログイン先７宛に回答する。この回答はゲートウェイ８で中継されて通信手段１に送られる。

【００１３】この通信手段１はゲートウェイ８に到る通信路、すなわちＬＡＮ１、のセキュリティレベルを符号４１で示す流れによりセキュリティ取得手段４に送り、次にゲートウェイ８，９からの回答を符号４１で示す流れによりセキュリティ取得手段４に送る。セキュリティ取得手段４は送られてきたセキュリティレベルのうち最低のレベルのものをログイン要求元１０からログイン先７に到る通信路のセキュリティレベルとして符号４２で

5

示す流れにより実行制御手段５に送る。

【００１４】ログイン許可の信号を受けたログイン要求元１０は通信路を経由しコマンドを送ってくる。このコマンドは通信手段１を経て符号１２で示す信号の流れにより実行制御手段５に入力される。実行制御手段５は当該コマンドの実行に要求されるセキュリティレベルをセキュリティレベル記憶手段６から読み出し、これとログイン手段２から送られる当該ログイン名のセキュリティレベルおよびセキュリティ取得手段４から送られる当該通信路のセキュリティレベルとを比較し、当該コマンドの実行を許可しまたは当該コマンドの実行を禁止する。

【００１５】

【発明の効果】以上説明したように本発明により通信路に応じたセキュリティレベルを得てそれに対応したセキュリティ保護を得ることができるので、ログイン要求元には要求元の性格によって定まる固定のログイン名を付与することができ、運用が容易になるという効果が得られる。

6

【図面の簡単な説明】

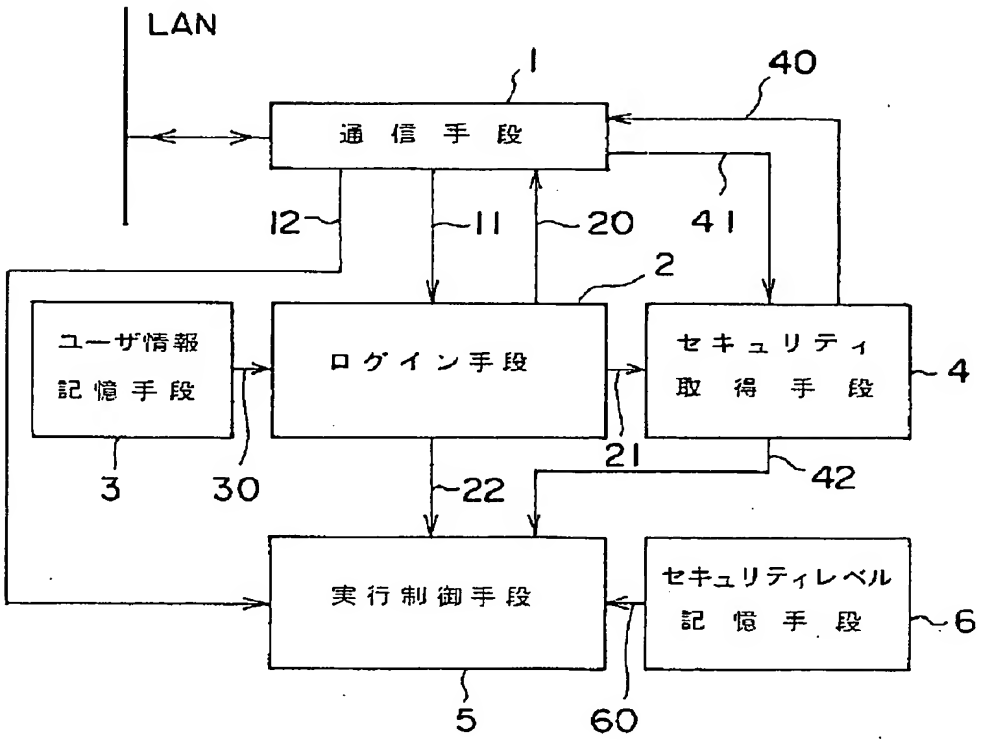
【図１】本発明の一実施例を示すブロック図である。

【図２】ログイン要求元からログイン先に到る通信路の構成を示すブロック図である。

【符号の説明】

１　通信手段
２　ログイン手段
３　ユーザ情報記憶手段
４　セキュリティ取得手段
５　実行制御手段
６　セキュリティレベル記憶手段
７　ログイン先
８　ゲートウェイ
９　ゲートウェイ
１０　ログイン要求元

【図１】



【図2】